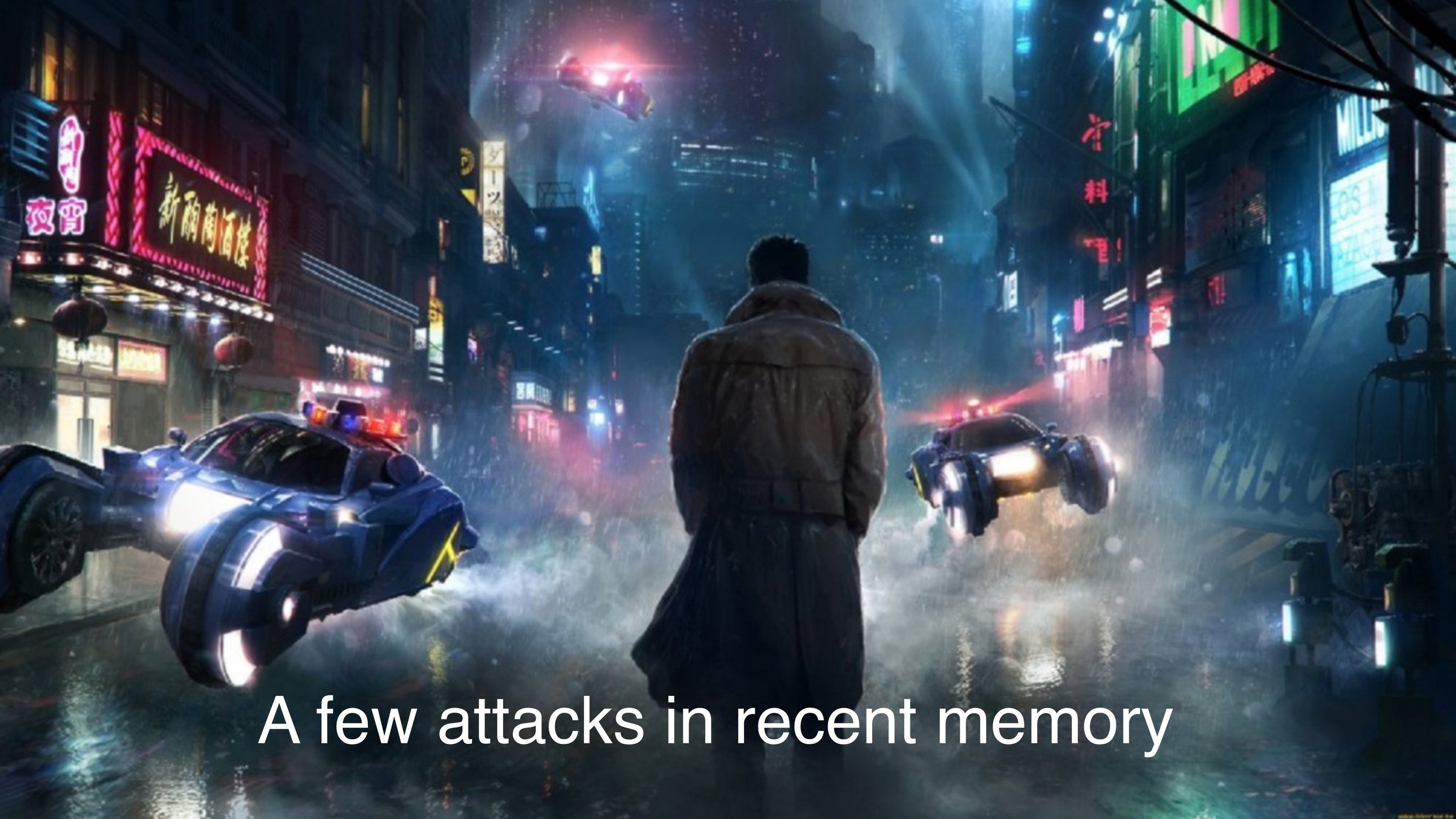
Security for the End User

Ben Whaley
bwhaley@kountable.com
@iAmTheWhaley

kountable™



A few attacks in recent memory

In 2010, the highly sophisticated Stuxnet worm, developed by Israel and US governments, was discovered by security researchers. It was designed to interrupt the Iranian nuclear program by attacking centrifuges.

Source of attack: Infected USB device

In 2013, ransomware attacks emerged in which private data is encrypted and held hostage for payment in Bitcoin. In 2017, damage due to ransomware estimated at $5B*

Source of attacks: Malware

*According to Cybersecurity Ventures

In 2015, the US Office of Personnel Management was breached, exposing sensitive details of 21M US citizens, many of whom held DoD security clearances.

Source of attacks: Unclear; probably phishing + weak authentication

In 2016, Russian state-sponsored hackers attacked the US election process, influencing the outcome and threatening the democratic process.

Source of attacks: Social engineering

In 2018, the Olympic opening ceremony was disrupted by Russian cyberattacks.

Source of attacks: Malware, probably achieved by phishing

Myth: You are too small to be a target

ATTN: For Your Perusal And Approval

Inbox x

Christopher Hale <kima279@aol.com>

to CraigAllen

9:25 AM (39 minutes ago)

"Christopher Hale" has never corresponded with you using this email address. Be careful with this message. Learn more

Hi Craig

Quick one..

Kindly review and approve. Office documents shared with you via https://docusign.kountable.com/statement/finance/pdf

Regards,
Christopher Hale

...../Outlook/...2017

People (2)

Christopher Hale

kima279@aol.com

Show details

Myth: Most attacks are outside of our control

99% of financial fraud emails relied on end-user clicks rather than automated exploits for malware installation

99% of attachment-based phishing attacks were launched by user clicks instead of automated exploits

78% of people claim to be aware of the risks of unknown links in emails and yet they click anyway

49% of US government agency security breaches are caused by a lack of user compliance

1

Identify malicious email and websites

- Messages with mismatched URLs
- URLs with misleading domain names
- Unfamiliar email addresses
- Messages asking for personal information
- Unexpected attachments

2

Strong authentication practices

- Protect critical accounts with multiple factors
- Use a password manager
- PIN codes for mobile devices
- Do not use SMS for anything sensitive

3 Basic computer security hygiene

- Keep software up-to-date
- Enable the local firewall
- Encrypt storage devices
- Exercise caution when downloading software
- Use secure network connections
- Antivirus software is not a panacea

4

Report suspicious activity

- Learn (or create) reporting procedures
- Centrally track security incidents
- Speak up and speak out
- Watch out for each other

5

Organizational commitment

- Centralized directory/Single sign-on
- Managed endpoint configuration
- Phishing campaigns and security awareness
- Responsive and approachable

Homework

- Enable MFA for personal accounts
- Select and embrace a password manager
- Implement basic security hygiene